EUR Form
セキュリティターゲット

2006/11/10

Version 1.06

(株)日立製作所

「EUR Form セキュリティターゲット」
― 変更歴 ―

項番	作成／変更年月日	ST バージョン	更新内容　（概要）	作成／変更者
1	2006/07/07	1.00	新規作成	谷口
2	2006/07/28	1.01	認証者とのキックオフ会議の結果を反映	谷口
3	2006/08/25	1.02	OR ASE-001-01,ASE-002-01 を反映	山田
4	2006/08/30	1.03	誤記訂正	山田
5	2006/09/25	1.04	OR ASE-003-01,ASE-004-01,ASE-005-01 を反映	山田
6	2006/10/26	1.05	OR ASE-006-01 を反映	山田
7	2006/11/10	1.06	認証レビュー CRV-T083-004 に対応	山田

■ 商標類

- Microsoft は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
- Microsoft Internet Explorer は，米国 Microsoft Corp. の商品名称です。
- Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
- Windows NT は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
- Windows Server は，米国およびその他の国における米国 Microsoft Corp. の商標です。

■ 著作権

「EUR Form セキュリティターゲット」

― 目次 ―

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合、用語の定義について記述する。

1.1. ST 識別

タイトル： EUR Form セキュリティターゲット
バージョン： 1.06
発行日： 2006 年 11 月 10 日
作成者： 株式会社　日立製作所　ソフトウェア事業部
TOE : EUR Form Client および EUR Form Client - Signature Option
TOE のバージョン： EUR Form Client 05-07
EUR Form Client - Signature Option 05-04
キーワード： 電子フォームシステム、 XML 署名、署名付与、署名検証
CC のバージョン：Common Criteria for Technology Security Evaluation Ver2.3
補足-0512 適用

1.2. ST 概要

本ドキュメントは、紙帳票と同じイメージで Web 画面に帳票を表示し，データの入力およびサーバへの送信ができるシステムである電子フォームシステムにおいて、電子的な帳票入力のためのソフトウェア製品である EUR Form Client および EUR Form Client - Signature Option のセキュリティターゲットである。

TOE は、電子フォームシステムのクライアント実行環境で利用するソフトウェアであり、TOE を利用することにより,入力画面が帳票イメージのように見やすく,用紙に記入するのと同じ感覚で EUR Form 帳票にデータを入力できる。また、入力したデータに対して、XML 署名を付与，および検証することができる。

TOE は，次に示す機能を提供する。

[メイン機能]

- EUR Form 帳票の表示
- EUR Form 帳票への申請データの入力
- EUR Form 帳票の印刷
- EUR Form 帳票のローカルディスクへの保存
- サーバへの申請データの送信

[セキュリティ機能]

- XML 署名の付与
- XML 署名の検証
- HTTPS 通信の開始

XML 署名が必要かどうか、データ送信時に HTTPS 通信が必要かどうかは、EUR Form 帳票定義時に、当該電子フォームシステムのセキュリティポリシーとして、電子フォームシステム設計者が EUR Form 帳票に設定する。TOE は、このポリシーに従い、上述したセキュリティ機能を具備することにより、エンドユーザが入力したデータの改ざん検出・通信路上の暴露防止という効果を発揮する。

1.3. CC 適合の主張

この ST は以下の CC に適合している。

- CC パート２拡張
- CC パート３適合

評価保証レベルは、EAL2＋ALC_FLR.1

1.4. 参考資料

- Common Criteria for Information Technology Security Evaluation Part 1:
  Introduction and general model August Version 2.3
  CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation Part 2:
  Security functional requirements August 2005 Version 2.3
  CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation Part 3:
  Security assurance requirements August 2005 Version 2.3
  CCMB-2005-08-003
- Common Methodology for Information Technology Security Evaluation
  Evaluation Methodology August 2005 Version 2.3
- 情報技術セキュリティ評価のためのコモンクライテリア パート 1：
  概説と一般モデル 2005 年 8 月 バージョン 2.3 CCMB-2005-08-001
  平成 17 年 12 月翻訳第 1.0 版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア パート 2：
  セキュリティ機能要件 2005 年 8 月 バージョン 2.3 CCMB-2005-08-002
  平成 17 年 12 月翻訳第 1.0 版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア パート 3：
  セキュリティ保証要件 2005 年 8 月 バージョン 2.3 CCMB-2005-08-003
  平成 17 年 12 月翻訳第 1.0 版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のための共通方法
  評価方法 2005 年 8 月 バージョン 2.3 CCMB-2005-08-004
  平成 17 年 12 月翻訳第 1.0 版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- [ガイドライン] 地方公共団体における申請・届出等手続に関する汎用受付システムの
  基本仕様(第二版)
  平成 15 年 3 月 28 日 自治事務等オンライン化推進関係省庁連絡会議
- [ガイドライン] 汎用受付システム構築の参考資料(調達編・共同方式の場合) (第 1.2 版)
  平成 16 年 3 月 総務省
- [ST] Microsoft Windows 2003/XP Security Target Version 1.0
  Microsoft Corporation, 28 September 2005

1.5. 用語

1.5.1. 本 ST における用語

用語	定義内容
電子フォームシステム	紙帳票と同じイメージで Web 画面に帳票を表示し，データの入力およびサーバへの送信ができるシステム
EUR Form 帳票	電子フォームシステム設計者が設計する帳票ファイル。記入すべき項目、Sign 帳票コントロール、送信ボタンなどの各種コントロールが設定されている。当該電子フォームシステムで使用する。
Sign 帳票コントロール	XML 部分署名を付与する際に設定する署名用コントロール。
電子フォームシステム設計者	当該電子フォームシステムのセキュリティポリシーの設計を行なう者。
申請者	EUR Form Client および EUR Form Client － Signature Option を利用して当該電子フォームシステムを利用して申請を行なう者。
審査者	EUR Form Client および EUR Form Client － Signature Option を利用して申請者の申請情報を検証する者。

1.5.2. 略語

<CC 関連略語>

CC（Common Criteria）：コモンクライテリア

EAL（Evaluation Assurance Level）：評価保証レベル

IT（Information Technology）：情報技術

PP（Protection Profile）：プロテクションプロファイル

SF（Security Function）：セキュリティ機能

SFP（Security Function Policy）：セキュリティ機能ポリシー

SOF（Strength Of Function）：機能強度

ST（Security Target）：セキュリティターゲット

TOE（Target Of Evaluation）：評価対象

TSC（TSF Scope of Control）：TSF 制御範囲

TSF（TOE Security Functions）：TOE セキュリティ機能

TSP（TOE Security Policy）：TOE セキュリティポリシー

<TOE 関連略語>

OS（Operating System）：基本ソフト

PKCS（Public Key Cryptography Standards）：RSADSI 社が定める、公開鍵暗号技術をベースとした各種の規格群。

RSA（Rivest Shamir Adleman）：Ronald Rivest 氏、Adi Shamir 氏、Leonard Adleman 氏の 3 人が 1978 年に開発した公開鍵暗号方式

HTTPS：SSL の暗号化通信を HTTP に実装したもの。Web ブラウザと Web サーバ間で，通信内容の盗聴，改ざん，漏えいなどの危険性を回避できる。

SSL（Secure Socket Layer）：Netscape Communications 社が開発した、インターネット上で情報を暗号化して送受信するプロトコル。

Web：WWW（World Wide Web）と同義。主に HTML（Hyper Text Markup Language）と呼ばれるマークアップ言語で記述された Web ページを Web サーバから読み出し、Web ブラウザで閲覧する技術。

CSP（Cryptographic Service Provider）：Microsoft(R) 社は，暗号エンジンを OS に組み込むときに，柔軟性と拡張性を重視して，暗号化ベンダがそれぞれプラグインできるオープン API を提供している。これらのプラグイン暗号エンジンを CSP という。

EUR（End-User Reporting）

2. TOE 記述

本章では、TOE 概要、TOE 関連の利用者役割、TOE 機能の論理的範囲、TOE の物理的範囲及びTOE 資産について記述する。

2.1. TOE の概要

2.1.1. TOE 種別

TOE は、電子フォームシステムにおいて、電子的な帳票入力を行なうためのソフトウェア製品であり、EUR Form 帳票の表示・EUR Form 帳票へのデータ入力・印刷・ローカルディスクへの保存、サーバへの申請データ送信機能および申請データの改ざんを検出するためのセキュリティ機能（XML 署名の付与・検証機能)、サーバに送信した申請データを通信路上の暴露から保護するためのセキュリティ機能（HTTPS 通信の開始機能）を提供する。

2.1.2. TOE を利用したシステム概要

TOE を利用したシステム概要および TOE を利用した業務の流れを図 2-1 に示す。
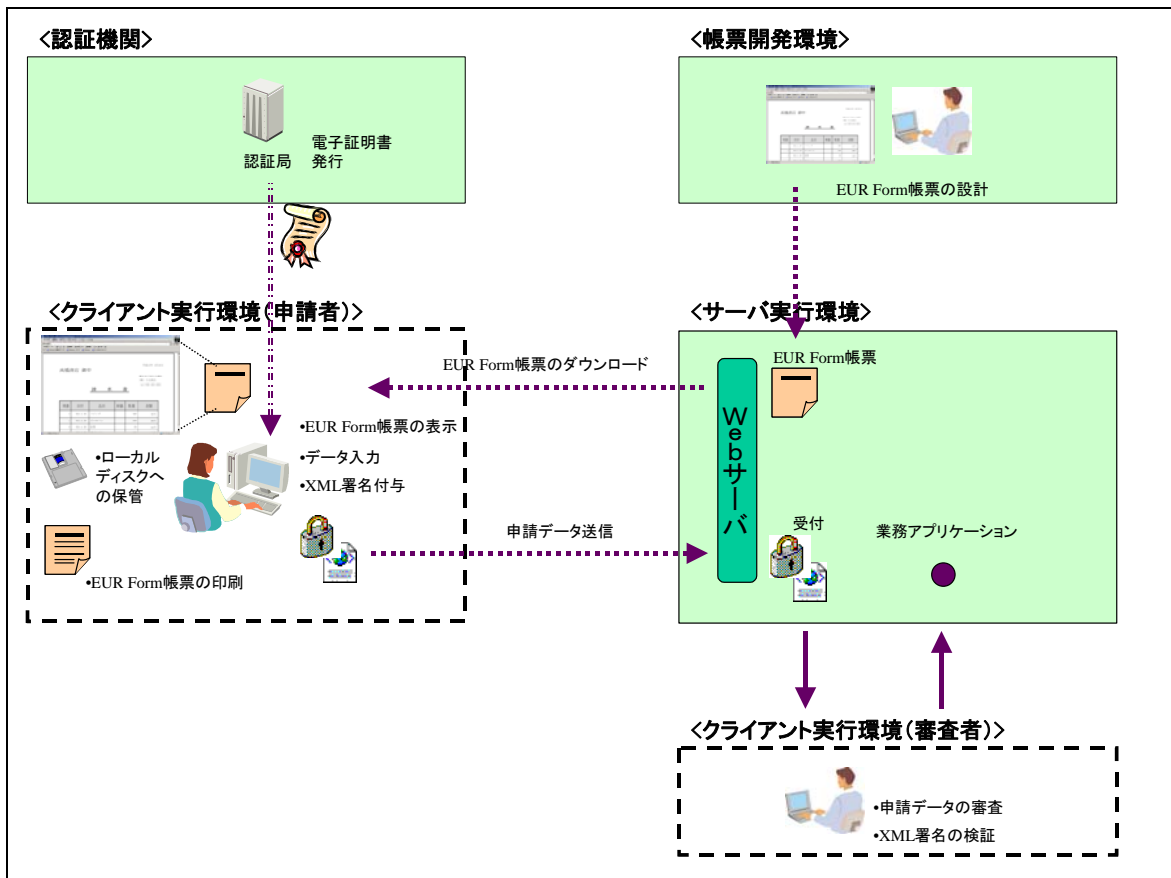
図 2-1 TOE を利用したシステム概要

図 2-1 に示したシステムを構成する構成要素について説明する。

【 認証機関 】

当該電子フォームシステムで必要な電子証明書を発行する。電子フォームシステム設計者が、認証機関の指定を行なう。認証機関は、TOE の範囲外である。

【 帳票開発環境 】

当該電子フォームシステムで利用する EUR Form 帳票を設計する。帳票開発環境は、TOE の範囲外である。

【 クライアント実行環境（申請者） 】

EUR Form 帳票の表示，申請データ入力、XML 署名の付与および入力した申請データをサーバへ送信する。また、必要に応じて EUR Form 帳票のローカルディスクへの保存および印刷を行なう。

クライアント実行環境（申請者）は TOE である。

【 クライアント実行環境（審査者） 】

申請者が付与した XML 署名の検証を行なう。クライアント実行環境（審査者）は TOE である。

【 サーバ実行環境 】

Web サーバを介して、申請者に対する EUR Form 帳票および TOE のダウンロード、申請者からの申請データの受付、審査者に対する申請データのダウンロードなどを行なう。

サーバ実行環境は、TOE の範囲外である。

図 2-1 に示したシステムにおける申請業務の流れを以下に示す。

- 申請者は、あらかじめ当該電子フォームシステムで指定された認証機関から電子証明書を申請・取得しておくものとする。
- 電子フォームシステム設計者は、当該電子フォームシステムで利用する EUR Form 帳票を設計する。その際、XML 署名が必要かどうか、HTTPS 通信が必要かどうかに関するセキュリティポリシーを決定し、EUR Form 帳票に設定する。
- 電子フォームシステム設計者は、作成した EUR Form 帳票および TOE をサーバ実行環境に登録する。
- 申請者は、TOE をサーバ実行環境からダウンロードし、インストールする。
- 申請者は、当該電子フォームシステムの EUR Form 帳票を、Web ブラウザを用いてダウンロードする。
- TOE は、ダウンロードされた EUR Form 帳票を表示する。
- 申請者は、EUR Form 帳票に当該電子フォームシステムで指定された申請データを入力する。
- 申請者は、必要に応じて EUR Form 帳票のローカルディスクへの保管・EUR Form 帳票の印

刷などを行なう。

- 申請者は、当該電子フォームシステムのセキュリティポリシーで指定されていた場合、XML 署名を付与する。
- 申請者は、申請データの入力・XML 署名付与の後、申請データをサーバに送信する。その際、当該電子フォームシステムのセキュリティポリシーで指定されていた場合、TOE は、送信する申請データに対して XML 署名を付与し、また HTTPS 通信の開始を指示する。
- 送信した申請データは、サーバ実行環境で受け付けられる。
- 審査者は、サーバ実行環境から Web ブラウザを用いて申請データをダウンロードする。
- 審査者は、申請データの確認および XML 署名の検証を行なう。

2.2. TOE 関連の利用者役割

TOE の利用者及び TOE に関連する役割を以下に示す。TOE の利用者は、申請者および審査者であり、TOE に関連する役割として、当該電子フォームシステムのセキュリティポリシーを決定するのが電子フォームシステム設計者である。

【申請者】

クライアント実行環境(申請者)において、以下の操作を行なう。

- EUR Form 帳票の Web ブラウザを用いたダウンロード
- EUR Form 帳票への申請データの入力
- 当該電子フォームシステムのセキュリティポリシーで指定されていた場合、署名対象データへの XML 署名の付与
- サーバへの申請データの送信

また、必要に応じて以下の操作を行なう。

- EUR Form 帳票の印刷
- EUR Form 帳票のローカルディスクへの保存

【審査者】

クライアント実行環境(審査者)において、以下の操作を行なう。

- サーバ実行環境で受け付けられた署名付き申請データ及び EUR Form 帳票の Web ブラウザを用いたダウンロード
- 申請データの内容の確認
- 申請者によって付与された XML 署名の検証

【電子フォームシステム設計者】

この役割は、TOE を直接操作する者ではないが、当該電子フォームシステムを構築・運用し、また当該電子フォームシステムに責任を持つものである。具体的には以下の作業を行なう。

- 以下に示すセキュリティポリシーの設計を行ない、EUR Form 帳票に設定を行なう。
  - ➢ 申請者による XML 署名の有無及び XML 署名の対象データ
  - ➢ サーバに送信する申請データ全体に対する XML 署名の有無
  - ➢ 申請データ送信時の HTTPS 通信使用の有無
- セキュリティポリシーを設定した EUR Form 帳票および TOE を当該電子フォームシステムの Web サーバに登録し、これらをセキュアにダウンロードさせるための手段を講じる。

2.3. TOE の論理的範囲

本 TOE は、紙帳票と同じイメージで Web 画面に帳票を表示し，データの入力およびサーバへの送信ができるシステムである電子フォームシステムにおいて、電子的な帳票入力のためのソフトウェア製品である。本 TOE で提供される機能は、以下に大別される。

[メイン機能]

- EUR Form 帳票の表示機能
- EUR Form 帳票への申請データの入力機能
- EUR Form 帳票の印刷機能
- EUR Form 帳票のローカルディスクへの保存機能
- サーバへの申請データの送信機能

[セキュリティ機能]

- XML 署名の付与機能
- XML 署名の検証機能
- HTTPS 通信の開始機能

2.3.1. TOE によって提供されるメイン機能

表 2-1 に、TOE が提供するメイン機能とその概要を示す。

表 2-1 TOE が提供するメイン機能

機能	概要
EUR Form 帳票の表示	申請者が Web ブラウザを用いてダウンロードした、あるいはダウンロード後ローカルディスクへ保存した EUR Form 帳票を Web ブラウザ上に表示する。
EUR Form 帳票への申請データの入力	申請者が入力する申請データを受け付ける。
EUR Form 帳票の印刷	EUR Form 帳票を申請者が入力した申請データと伴に印刷することができる。
EUR Form 帳票のローカルディスクへの保存	申請者が申請データの入力途中の場合、あるいはサーバへ送信する申請データの控えとして、ローカルディスクへ保存することができる。
サーバへの申請データの送信	申請者による入力が完了した申請データを、電子フォームシステムによって指定されたサーバに送信する。

2.3.2. TOE によって提供されるセキュリティ機能

【XML 署名の付与機能】

(1) メッセージ署名機能

EUR Form 帳票にメッセージ署名機能を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOE は、申請者がサーバに送信する申請データ全体を署名対象として XML 署名を付与する機能を提供する。

(2) 部分署名機能

EUR Form 帳票に部分署名機能を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOE は、EUR Form 帳票に設定されている署名対象データに対して XML 署名を付与する機能を提供する。

XML 署名の付与機能において、署名形式は、PKCS#1 形式、署名アルゴリズムは、SHA-1 RSA を使用する。

また、サーバに申請データを送信する前に、記入内容の誤りに気付いた場合など、部分署名を付与した者であれば、当該部分署名を解除し、記入訂正を行なうことができる。

【XML 署名の検証機能】

申請データに部分署名が付与されていた場合、TOE は審査者が、当該部分署名を検証する機能を提供する。本機能により、審査者は、当該部分署名が付与された以降に、当該部分署名の署名対象データに改ざんが行なわれたか否かを確認することができる。

【HTTPS 通信の開始機能】

EUR Form 帳票に HTTPS 通信を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOE は、Windows Platform に対して HTTPS 通信の開始を指示する機能を提供する。

2.3.3. TOE によって提供されないセキュリティ機能

XML 署名の付与機能において、XML 署名に使用する電子証明書は、TOE の利用開始前にあらかじめ当該電子フォームシステムで指定された認証機関に申請者が申請・取得しておくものとする。

XML 署名に使用する電子証明書の配布形態は、当該電子フォームシステムで指定された認証機関の配布形態によって決定されるが、以下の 2 通りが一般的である。

- フロッピーディスクなどで配布される。申請者は、TOE の利用開始前に、入手した電子証明書を Windows Platform の証明書ストアに格納しておく。
- IC カードに格納された形式で、IC カードアクセスのための専用ソフトウェアとともに配布される。

TOE は、上述したようにメッセージ署名機能、部分署名機能を提供するが、具体的な暗号アルゴリ

ズムの実装、電子証明書のハンドリング、IC カードへのアクセスに関する機能は、Windows の機能、あるいは専用ソフトウェアの機能であり、TOE の範囲外である。

TOE は、上述したように HTTPS 通信の開始機能を提供するが、具体的な HTTPS 通信の実装は、Windows の機能であり、TOE の範囲外である。

2.4. TOE の物理的範囲

2.4.1. TOE の物理的範囲

第 2.1.2 節で記述したように、TOE が稼動する端末は、図 2-1 において破線内で示した<クライアント実行環境（申請者）>および<クライアント実行環境（審査者）>が TOE の稼動する端末である。

図 2-2 に TOE の物理的範囲を示す。
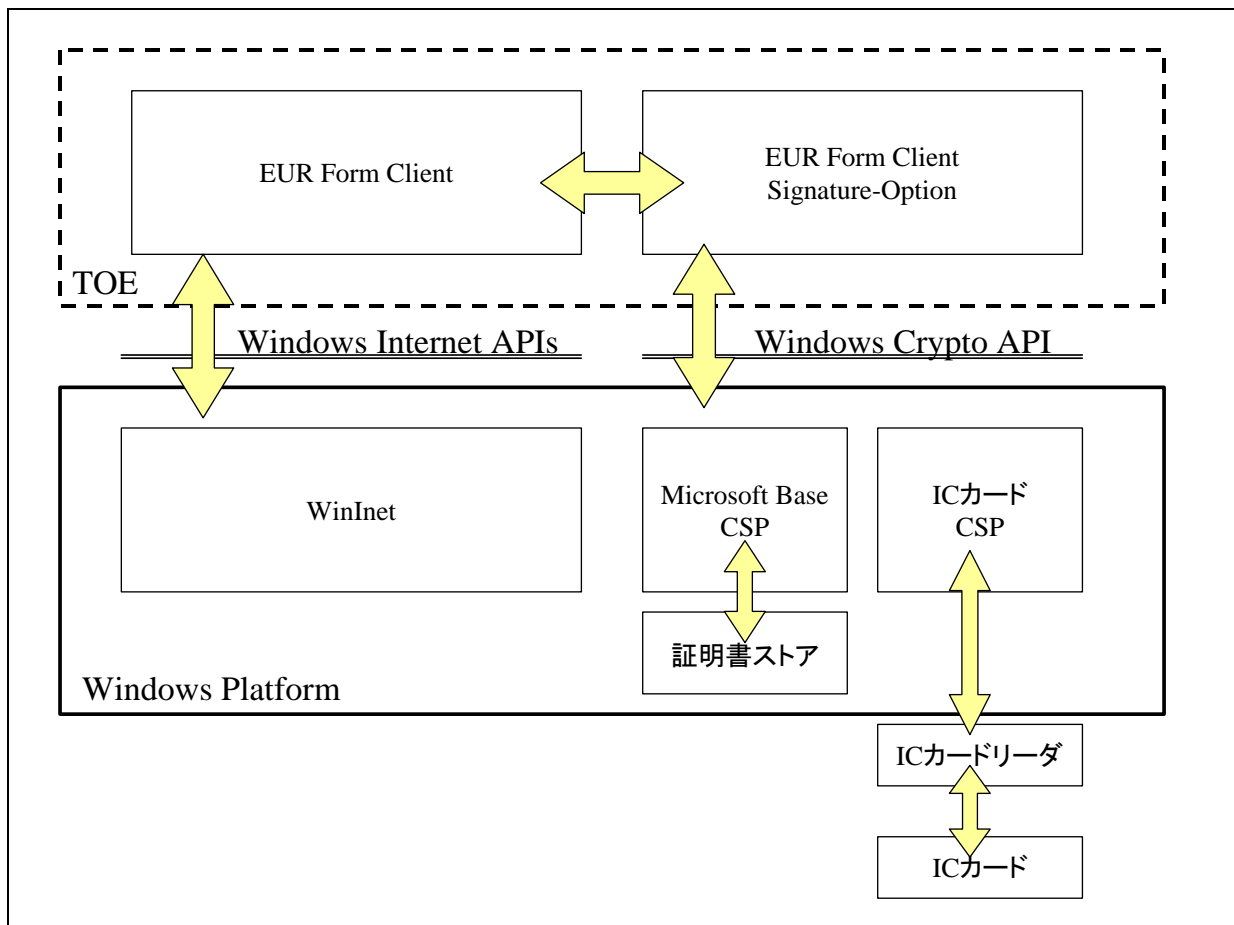
図 2-2 TOE の物理的範囲

図 2-2 の破線内で示したコンポーネントである EUR Form Client および EUR Form Client – Signature Option が、TOE の物理的範囲内である。

TOE は、Windows Platform が提供する Windows Crypto API を介し Cryptographic Service Provider(CSP)を用いて、署名付与、署名検証を行なう。Windows Platform の証明書ストアを使用する場合、Windows Platform が提供する Microsoft Base CSP を利用する。

IC カードを使用する場合、IC カードアクセスのための専用ソフトウェアが提供する IC カード CSP を利用する。

TOE は、Windows Platform が提供する Windows Internet APIs を介し、WinInet に対して HTTPS 通信の開始を指示する。

2.4.2. ハードウェア条件

表 2-2 に、TOE の動作環境としてのハードウェア条件を示す。TOE は、表 2-2 を満たす動作環境で、正しく確実に動作する。

表 2-2 ハードウェア条件

端末名	種別	説明
クライアント実行環境(申請者)および(審査者)		
本体		
	本体マシン	表 2-3 に示す OS が動作する PC/AT 互換機
	CPU	Intel® Celeron プロセッサ 1GHz 以上
	メモリ	512MB 以上
	HDD	20GB 以上
IC カードリーダ ※電子証明書が IC カードに格納されている場合に使用する		
	「公的個人認証に対応する IC カードリーダライタ」	

「公的個人認証に対応する IC カードリーダライタ」は、財団法人 自治体衛星通信機構 公的個人認証サービスセンターが仕様公開及び適合性検証を実施している。

2.4.3. ソフトウェア条件

表 2-3 に TOE が稼動するためのソフトウェア条件を示す。

表 2-3 ソフトウェア条件

ベンダ名	製品名	説明
クライアント実行環境		
Microsoft	Windows XP Professional SP2 以降	OS
Microsoft	Internet Explorer Version 6.0 以降	Web ブラウザ
(株)日立製作所	EUR Form Client 05-07	TOE
(株)日立製作所	EUR Form Client – Signature Option 05-04	TOE
公的個人認証サービス 指定認証機関 財団法人 自治体衛星通信機構	公的個人認証サービス 利用者クライアントソフト 平成 17 年 10 月版	IC カードに格納された電子証明書を利用する場合に使用する。

公的個人認証サービス 利用者クライアントソフト は、IC カードに格納された公的個人認証サー

ビスの電子証明書を利用するためのソフトウェアであり、公的個人認証サービスを利用した電子申請を行なうために必要となるソフトウェアである。

IC カードに格納された公的個人認証サービスの電子証明書の発行を受けた際に、市区町村の窓口にて CD-ROM 形式で渡される。

図 2-2 の IC カード CSP と示したコンポーネントは、本ソフトウェアに格納されている。

2.5. TOE の資産

本 TOE の資産は、申請者が EUR Form 帳票へ入力する申請データである。

また、本 TOE のセキュリティ機能を駆動するか否かを決定するデータとして、電子フォームシステム設計者が設定する以下のデータが EUR Form 帳票内に格納されている。

- 申請者が XML 署名を付与するかどうか
- 申請者が付与する XML 署名の対象データ
- サーバに送信する申請データ全体に XML 署名を付与するかどうか
- 申請データの送信時に HTTPS 通信を行なうかどうか

上述したように、本 TOE は、TOE の範囲外である帳票開発環境において、TOE 外の利用者である電子フォームシステム設計者が設定したセキュリティポリシーに従い、申請者が入力した申請データの改ざん検出・通信路上の暴露防止という効果を発揮するセキュリティ機能を具備した製品である。これら TOE の性質を考え、TOE としてこれらのデータに対する脅威は存在せず、TOE の直接の保護対象ではないものとする。

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティポリシーについて記述する。

本 TOE は、当該電子フォームシステムの設計者が EUR Form 帳票に設定したセキュリティポリシーを実現するためにセキュリティ機能を具備している。TOE のセキュリティ機能により、セキュリティポリシーとして EUR Form 帳票に設定されている場合、申請者が入力した申請データの改ざん検出、および申請者が送信した申請データの通信路上の暴露防止という効果が発揮される。

従って、TOE が想定する脅威は存在せず、また、第 3.3 節に示す組織のセキュリティポリシーを実現するために必要な前提条件を第 3.1 節に記述する。

3.1. 前提条件

第 3.3 節に示す組織のセキュリティポリシーを実現するために TOE のセキュリティ機能が有効に働くためには、TOE のセキュリティ機能が利用する EUR Form 帳票、電子証明書および TOE が動作する IT 環境が正当なものであることが条件となる。

従って、以下を TOE の前提条件としてあげる。

A. CERT_USE

申請者は、署名の付与に使用する電子証明書として、当該電子フォームシステムで既定された TOE 外の信頼できる認証機関によって発行された電子証明書を利用する。発行された電子証明書は信頼できるものとする。また、申請者は、この電子証明書を適切に管理し、申請データへの署名に使用する電子証明書を正しく選択するものとする。

A. EUR_FORM

電子フォームシステム設計者は、当該電子フォームシステムのセキュリティを考慮し、適切なセキュリティポリシーを EUR Form 帳票に設定するものとする。また、電子フォームシステム設計者は、適切なセキュリティポリシーが設定された EUR Form 帳票を当該電子フォームシステムの Web サーバに登録し、TOE の利用者に対してセキュアにダウンロードさせる。

A. IT_ENV

TOE が稼動するために使用するソフトウェアは、正しく動作するものとする。

3.2. 脅威

TOE が想定する脅威は存在しない。

3.3. 組織のセキュリティポリシー

P. SIGN
当該電子フォームシステムにおいては、申請データに対して署名を付与すること。

P. VERIFY
当該電子フォームシステムにおいては、電子証明書に格納されている公開鍵を用いて、申請データに付与された署名を検証し、申請データの改ざんチェックを行なうこと。

P.SECURE_CHANNEL
当該電子フォームシステムにおいて、申請データの送信を行なう場合、HTTPS を使用し、通信経路の暗号化を行なうこと。

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針、環境セキュリティ対策方針について記述する。

4.1. TOE セキュリティ対策方針

O. SIGN

TOE は、当該電子フォームシステムで既定されたセキュリティポリシーに従い、申請データに対して XML 署名を付与する機能を提供しなければならない。

O. VERIFY

TOE は、当該電子フォームシステムで既定されたセキュリティポリシーに従い、申請者が付与した部分署名を審査者が検証する機能を提供しなければならない。

O.INITIATE_HTTPS

TOE は、当該電子フォームシステムで既定されたセキュリティポリシーに従い、申請データを送信するサーバとの間で HTTPS 通信を開始する機能を提供しなければならない。

4.2. 環境セキュリティ対策方針

OE.CRYPTO

IT 環境は、TOE からの要求に従って、暗号操作機能を提供しなければならない。

OE.SECURE_CHANNEL

IT 環境は、TOE からの要求に従って、申請データを送信するサーバとの間で HTTPS を使用した暗号通信機能を提供しなければならない。

OM.CERT_MANAGE

申請者は、あらかじめ当該電子フォームシステムで定められた手順に則り、指定された認証機関から署名に使用する電子証明書を取得しなければならない。また、申請者は、TOE のガイダンス文書に従って、取得した電子証明書を適切に管理しなければならない。

OM.SIGNER

申請者は、TOE のガイダンス文書に従って、当該電子フォームシステムで既定された電子証明書を使用して、申請データに署名を付与しなければならない。

OM.VERIFIER

審査者は、TOE のガイダンス文書に従って、申請データに付与された署名を検証し、申請データの改ざんをチェックしなければならない。

OM.EUR_FORM

電子フォームシステム設計者は、当該電子フォームシステムで既定された手順に則り、既定されたセキュリティポリシーを、適切に EUR Form 帳票に設定しなければならない。
また、電子フォームシステム設計者は、適切なセキュリティポリシーが設定された EUR Form 帳票を当該電子フォームシステムの Web サーバに登録し､TOE の利用者に対してセキュアにダウンロードさせなければならない。

OM.MAINTENANCE

TOE の利用者は、OS のパッチを定期的に適用するなど、TOE が動作するためにソフトウェアの適切な管理を行なわなければならない。

5. IT セキュリティ要件

本章では、TOE セキュリティ要件、IT 環境セキュリティ要件について記述する。

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

TOE が提供するセキュリティ機能の機能要件を記述する。本 ST では、TSF 間高信頼チャネルの開始に関する機能要件コンポーネントとして CC パート 2 で規定されている **FTP_ITC.1** を拡張し **FTP_ITC_EX_INI.1** を設けている。これ以外の機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用している。

FDP_DAU.1　基本データ認証
下位階層 ： なし

FDP_DAU.1.1　TSF は、[割付: オブジェクトまたは情報種別のリスト]の有効性の保証として使用できる証拠を生成する能力を提供しなければならない。
[割付: オブジェクトまたは情報種別のリスト]: 申請者がサーバに送信する申請データ全体および EUR Form 帳票に設定されている部分署名の対象データ

FDP_DAU.1.2　TSF は、示された情報の有効性の証拠を検証する能力を[割付: サブジェクトのリスト]に提供しなければならない。
[割付: サブジェクトのリスト] : 審査者
[詳細化] ：示された情報 →　EUR Form 帳票に設定されている部分署名の対象データ

依存性 ：　なし

FTP_ITC_EX_INI.1　TSF 間高信頼チャネルの開始
下位階層 ： なし

管理 : FTP_ITC_EX_INI.1
以下のアクションは FMT における管理機能と考えられる:
a) もしサポートされていれば、高信頼チャネルを要求するアクションの設定。

監査: FTP_ITC_EX_INI.1
FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象に

すべきである:

a) 最小: 高信頼チャネル機能の失敗。

b) 最小: 失敗した高信頼チャネル機能の開始者とターゲットの識別。

c) 基本: 高信頼チャネル機能のすべての使用の試み。

d) 基本: すべての高信頼チャネル機能の開始者とターゲットの識別。

FTP_ITC_EX_INI.1.1 TSF は、[選択: TSF、リモート高信頼 IT 製品]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

[選択: TSF、リモート高信頼 IT 製品] : TSF

FTP_ITC_EX_INI.1.2 TSF は、[割付: 高信頼チャネルが要求される機能のリスト]のために、高信頼チャネルを介して通信を開始しなければならない。

[割付: 高信頼チャネルが要求される機能のリスト] : 当該電子フォームシステムのセキュリティポリシーとして既定されていた場合、申請データの送信

依存性 : なし

5.1.2. 最小機能強度レベル

本 TOE の最小機能強度レベルは、SOF-基本であるが、本 TOE において、確率的または順列的メカニズムに基づくセキュリティ機能要件はない。

5.1.3. TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL2 であり、追加する保証コンポーネントは ALC_FLR.1 である。すべての保証要件コンポーネントは、CC パート 3 で規定されている評価コンポーネントを直接使用する。EAL2＋ALC_FLR.1 の評価コンポーネントを表 5-1 に示す。

表 5-1 EAL2＋ALC_FLR.1 評価コンポーネント一覧

保証クラス	保証コンポーネント	
構成管理（ACM クラス）	**ACM_CAP.2**	構成要素
配付と運用（ADO クラス）	**ADO_DEL.1**	配付手続き
	ADO_IGS.1	設置、生成、及び立上げ手順
開発（ADV クラス）	**ADV_FSP.1**	非形式的機能仕様
	ADV_HLD.1	記述的上位レベル設計
	ADV_RCR.1	非形式的対応の実証
ガイダンス文書（AGD クラス）	**AGD_ADM.1**	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ライフサイクルサポート（ALC クラス）	**ALC_FLR.1**	基本的な欠陥修正
テスト（ATE クラス）	**ATE_COV.1**	カバレージの証拠
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
脆弱性評定（AVA クラス）	**AVA_SOF.1**	TOE セキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.2. IT 環境セキュリティ要件

IT 環境が提供するセキュリティ機能の機能要件を記述する。本 ST では、TSF 間高信頼チャネルの実装に関する機能要件コンポーネントとして CC パート 2 で規定されている **FTP_ITC.1** を拡張し **FTP_ITC_EX_IMP.1** を設けている。これ以外の機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用している。

FCS_COP.1 暗号操作

下位階層 ： なし

FCS_COP.1.1 TSF は、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: 暗号操作のリスト]を実行しなければならない。

[詳細化] ：TSF は、→ IT 環境は、

上述の割付を下表に示す。

暗号操作	標準	暗号アルゴリズム	暗号鍵長
CryptSignHash 関数	なし	FIPS-186-2 RSA using PKCS-1	最大 2048 bit
CryptCreateHash 関数 CryptHashData 関数 CryptGetHashParam 関数	FIPS180-2	FIPS-180-2 SHA-1	適用せず

依存性 ： [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FDP_ITC.2 セキュリティ属性付き利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4 暗号鍵破棄

下位階層 ： なし

FCS_CKM.4.1 TSF は、以下の[割付:標準のリスト]に合致する、指定された暗号鍵破棄方法[割付: 暗号鍵破棄方法]に従って、暗号鍵を破棄しなければならない。

［詳細化］：TSF は、→ IT 環境は、

上述の割付を下表に示す。

標準	暗号鍵破棄方法
FIPS 140-1 または FIPS 140-2 レベル 1	暗号鍵ゼロ化方法

依存性 ： [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FDP_ITC.2 セキュリティ属性付き利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FMT_MSA.2 セキュアなセキュリティ属性

FTP_ITC_EX_IMP.1 TSF 間高信頼チャネルの実装
下位階層 ： なし

管理：FTP_ITC_EX_IMP.1
以下のアクションは FMT における管理機能と考えられる:
a) もしサポートされていれば、高信頼チャネルを要求するアクションの設定。

監査: FTP_ITC_EX_IMP.1
FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:
a) 最小: 高信頼チャネル機能の失敗。
b) 最小: 失敗した高信頼チャネル機能の開始者とターゲットの識別。
c) 基本: 高信頼チャネル機能のすべての使用の試み。
d) 基本: すべての高信頼チャネル機能の開始者とターゲットの識別。

FTP_ITC_EX_IMP.1.1 TSF は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

［詳細化］：TSF は、→ IT 環境は、

依存性 ： なし

6. TOE 要約仕様

本章では、TOE の要約仕様を記述する。

6.1. TOE セキュリティ機能

本節では、TOE のセキュリティ機能を説明する。表 6-1 に示すように、本節で説明するセキュリティ機能は、第 5.1.1 節で記述した TOE セキュリティ機能要件を満たすものである。

表 6-1 TOE セキュリティ機能とセキュリティ機能要件の対応関係

TOE セキュリティ機能要件 ＼ TOE セキュリティ機能	FDP_DAU.1	FTP_ITC_EX_INI.1
SF.MESSAGE_SIGN	○	
SF.PARTIAL_SIGN	○	
SF.PARTIAL_VERIFY	○	
SF.INITIATE_HTTPS		○

6.1.1. XML 署名の付与機能

SF.MESSAGE_SIGN

EUR Form 帳票にメッセージ署名機能を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOE は、申請者がサーバに送信する申請データ全体を署名対象として XML 署名を付与する機能を提供する。

申請者が、EUR Form 帳票に設定された送信ボタンを押下することにより、本機能は起動する。EUR Form 帳票には、電子フォームシステム設計者がセキュリティポリシーに従い設定した 電子証明書の格納先が設定されている。

SF.PARTIAL_SIGN

EUR Form 帳票に部分署名機能を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOE は、EUR Form 帳票に設定されている署名対象データに対して XML 署名を付与する機能を提供する。

申請者が、EUR Form 帳票に設定された Sign 帳票コントロールを押下することにより、本機能は起動する。EUR Form 帳票には、電子フォームシステム設計者がセキュリティポリシーに従い設定した 、

署名対象データ、電子証明書の格納先が設定されている。

部分署名の付与に成功した場合、TOE は、EUR Form 帳票に設定された定義に従い、部分署名を付与した旨を示すマークを申請者に提示する。

部分署名の付与に使用した電子証明書を保持している場合、申請者は、Sign 帳票コントロールを操作することにより、一旦付与した部分署名を解除することができる。部分署名の解除に成功した場合、TOE は 部分署名を付与した旨を示すマークも解除する。

上述した 2 つのセキュリティ機能において、TOE は、IT 環境に格納された電子証明書を利用して、また、IT 環境の暗号操作機能を利用して XML 署名を付与する。

電子証明書の格納先として、Windows Platform の証明書ストアが指定されていた場合、TOE は、署名対象データを成形し Microsoft Base CSP を利用して署名データを生成する。

証明書ストアに複数の電子証明書が格納されていた場合、TOE は電子証明書を識別する情報を申請者に提示し、申請者は適切な電子証明書を選択する。TOE は、選択された情報で示される電子証明書を用いて、Microsoft Base CSP を利用して署名データを生成する。

電子証明書の格納先として、IC カードが指定されていた場合、TOE は、署名対象データを成形し IC カード CSP を利用して署名データを生成する。

6.1.2. XML 署名の検証機能

SF.PARTIAL_VERIFY

申請データに部分署名が付与されていた場合、TOE は審査者が、当該部分署名を検証する機能を提供する。

審査者が当該 Sign 帳票コントロールを操作することにより本機能は起動する。

当該 Sign 帳票コントロールの署名対象データに対する改ざんが検出された場合、TOE は、当該署名対象データが改ざんされた可能性がある旨、審査者に対して提示する。

当該 Sign 帳票コントロールの署名対象データに対する改ざんが検出されなかった場合、TOE は、当該署名対象データが署名付与後変更されていない旨、審査者に対して提示する。

本機能により、審査者は、当該部分署名が付与された以降に、当該部分署名の署名対象データに改ざんが行なわれたか否かを確認することができる。

TOE は、申請データに付与された部分署名の署名対象データを成形し、Microsoft Base CSP を利用して署名の検証を行なう。

6.1.3. HTTPS 通信の開始機能

SF.INITIATE_HTTPS

EUR Form 帳票に HTTPS 通信を有効とするような設定がセキュリティポリシーとしてなされていた場合、TOE は、申請データを送信するサーバとの間で HTTPS 通信を開始する機能を提供する。

TOE は、Windows Platform に対して HTTPS 通信の開始を指示する機能を提供する。

6.2. セキュリティ機能強度

本 TOE において、SOF 主張を実現すべき IT セキュリティ機能はない。

6.3. 保証手段

本節では、TOE のセキュリティ保証手段を説明する。表 6-2 に示すように、以下のセキュリティ保証手段は、第 5.1.3 節で記述した TOE セキュリティ保証要件を満たすものである。

表 6-2 保証手段と保証要件コンポーネントの対応関係

保証要件クラス	保証要件 コンポーネント	保証手段
ASE：ST 評価	**ASE_INT.1** **ASE_DES.1** **ASE_ENV.1** **ASE_OBJ.1** **ASE_REQ.1** **ASE_SRE.1** **ASE_TSS.1** **ASE_PPC.1**	EUR Form セキュリティターゲット
ACM：構成管理	**ACM_CAP.2**	EUR Form 構成管理文書
ADO：配付と運用	**ADO_DEL.1**	EUR Form 配付文書 電子フォームシステム EUR Form EUR Form サーバシステム構築 EUR Form セキュア取扱説明書
	ADO_IGS.1	電子フォームシステム EUR Form EUR Form Client クライアント操作 EUR Form セキュア取扱説明書 EUR Form Client ダウンロードサイト
ADV：開発	**ADV_FSP.1**	EUR Form 機能仕様書 EUR Form 詳細設計書 EUR Form 対応分析書
	ADV_HLD.1	EUR Form 詳細設計書
	ADV_RCR.1	EUR Form 対応分析書
AGD：ガイダンス文書	**AGD_ADM** **AGD_USR**	電子フォームシステム EUR Form EUR Form Client クライアント操作 EUR Form セキュア取扱説明書 EUR Form Client ダウンロードサイト
ALC：ライフサイクルサポート	**ALC_FLR.1**	EUR Form 欠陥修正規程書
ATE：テスト	**ATE_COV.1**	EUR Form テスト分析書
	ATE_FUN.1	EUR Form テスト仕様書／報告書
	ATE_IND.2	TOE
AVA：脆弱性評定	**AVA_SOF.1**	なし
	AVA_VLA.1	EUR Form 脆弱性分析書

7. PP 主張

本章では、PP 主張について記述する。

7.1. PP 参照

参照した PP はない。

7.2. PP 修整

修整した PP はない。

7.3. PP 追加

PP への追加はない。

8. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠について記述する。

8.1. セキュリティ対策方針根拠

セキュリティ対策方針は、TOE セキュリティ環境で既定した前提条件と組織のセキュリティポリシーを実現するためのものである。セキュリティ対策方針と対応する前提条件および組織のセキュリティポリシーの対応関係を表 8-1 に示す。

表 8-1 セキュリティ対策方針と対応する前提条件および組織のセキュリティポリシーの対応関係

前提条件 / 組織のセキュリティポリシー / セキュリティ対策方針	P.SIGN	P.VERIFY	P.SECURE_CHANNEL	A.CERT_USE	A.EUR_FORM	A.IT_ENV
O.SIGN	○					
O.VERIFY		○				
O.INITIATE_HTTPS			○			
OE.CRYPTO	○	○				
OE.SECURE_CHANNEL			○			
OM.CERT_MANAGE				○		
OM.SIGNER	○			○		
OM.VERIFIER		○				
OM.EUR_FORM					○	
OM.MAINTENANCE						○

＜根拠＞
表 8-1 により、TOE のすべてのセキュリティ対策方針は、組織の対策方針に対応している。
また、環境のセキュリティ対策方針は、組織のセキュリティ対策方針および前提条件に対応している。

本 TOE は、電子フォームシステムの設計者が EUR Form 帳票に設定する当該電子フォームシステ

ムの組織のセキュリティポリシーを実現するためにセキュリティ機能を具備している製品であり、組織のセキュリティポリシーは、以下の TOE のセキュリティ対策方針、および環境のセキュリティ対策方針で実現している。

P.SIGN：

O.SIGN により、TOE は申請者に対して、申請データに XML 署名を付与する機能を提供する。署名付与に関する実際の暗号操作は、**OE.CRYPTO** により TOE および IT 環境のセキュリティ対策方針が協力して対抗する。また、**OM.SIGNER** により、申請者は当該電子フォームシステムで既定された電子証明書を利用し、TOE を用いて適切に申請データに署名を付与することができる。以上により **P.SIGN** は、**O.SIGN**、**OE.CRYTO** 及び **OM.SIGNER** により実現できる。

P.VERIFY：

O.VERIFY により、TOE は審査者に対して、申請データに付与された部分署名を検証する機能を提供する。署名検証に関する実際の暗号操作は、**OE.CRYPTO** により TOE および IT 環境のセキュリティ対策方針が協力して対抗する。また、**OM.VERIFIER** により、審査者は当該電子フォームシステムで既定された手順に則り、TOE を用いて署名を検証し、申請データの改ざんチェックを行なうことができる。以上により **P.VERIFY** は、**O.VERIFY**、**OE.CRYTO** 及び **OM.VERIFIER** により実現できる。

P.SECURE_CHANNEL：

O.INITIATE_HTTPS により、TOE は申請データの送信を行なう際に HTTPS を使用した高信頼チャネルを開始する。HTTPS 通信に関する実際の通信経路の暗号操作は、**OE.SECURE_CHANNEL** により TOE および IT 環境のセキュリティ対策方針が協力して対抗する。以上により **P.SECURE_CHANNEL** は、**O.INITIATE_HTTPS** 及び **OE.SECURE_CHANNEL** により実現できる。

A.CERT_USE：

OM.CERT_MANAGE により、申請者は、あらかじめ当該電子フォームシステムで定められた手順に則り、指定された認証機関から署名に使用する電子証明書を取得する。また、申請者は取得した電子証明書は申請者が適切に管理する。さらに、**OM.SIGNER** により、申請者は、TOE のガイダンス文書に従って、取得した電子証明書を使用して、申請データに署名を付与する。

以上により、**A.CERT_USE** は、**OM.CERT_MANAGE** 及び **OM.SIGNER** により実現できる。

A.EUR_FORM：

OM.EUR_FORM により、電子フォームシステム設計者は、当該電子フォームシステムで既定された手順に則り、既定されたセキュリティポリシーを、適切に EUR Form 帳票に設定する。

また、電子フォームシステム設計者は、適切なセキュリティポリシーが設定された EUR Form 帳票を当該電子フォームシステムの Web サーバに登録し、TOE の利用者に対してセキュアにダウンロードさ

せる。
従って **A.EUR_FORM** は、**OM.EUR_FORM** により実現できる。

A.IT_ENV：
OM.MAINTENANCE により、TOE の利用者は、定期的に OS のパッチを適用するなどして、TOE が動作するためにソフトウェアの適切な管理を行なう。
従って、**A.IT_ENV** は、**OM.MAINTENANCE** により実現できる。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ機能要件根拠

セキュリティ機能要件とセキュリティ対策方針の対応関係を表 8-2 に示す。

表 8-2 セキュリティ機能要件とセキュリティ対策方針の対応関係

セキュリティ機能要件 ＼ セキュリティ対策方針	O.SIGN	O.VERIFY	O.INITIATE_HTTPS	OE.CRYPTO	OE.SECURE_CHANNEL
FDP_DAU.1	○	○			
FTP_ITC_EX_INI.1			○		
FCS_COP.1				○	
FCS_CKM.4				○	
FTP_ITC_EX_IMP.1					○

表 8-2 により、すべての TOE のセキュリティ機能要件は、TOE のセキュリティ対策方針に対応している。また、すべての IT 環境のセキュリティ機能要件は、IT 環境のセキュリティ対策方針に対応している。

O.SIGN：
TOE は、**FDP_DAU.1** により申請データの有効性の保証として使用できる証拠を生成する能力として、XML 署名を付与する機能を提供する。

O.VERIFY：
TOE は、**FDP_DAU.1** により申請データの有効性の証拠を検証する能力として、XML 署名を検証する機能を提供する。

O.INITIATE_HTTPS：
TOE は、**FTP_ITC_EX_INI.1** により高信頼チャネルを開始する機能を提供する。

以上により、すべての TOE セキュリティ対策方針に対して、何らかのセキュリティ機能要件が十分実

現している。

OE.CRYPTO：
IT 環境は、**FCS_COP.1** により指定された標準に基づくアルゴリズムと鍵長に従って、XML 署名の付与および検証のための暗号機能を提供する。
また、**FCS_CKM.4** により、**FCS_COP.1** で利用する鍵は安全に破棄される。

OE.SECURE_CHANNEL：
IT 環境は、**FTP_ITC_EX_IMP.1** により申請データを送信するサーバとの間で HTTPS を使用した通信機能を提供する。

以上により、すべての IT 環境のセキュリティ対策方針に対して、何らかのセキュリティ機能要件が十分実現している。

本 ST では、TSF 間高信頼チャネルの開始に関する機能要件コンポーネントとして、TOE のセキュリティ機能要件 **FTP_ITC_EX_INI.1** を設けている。また、TSF 間高信頼チャネルの実装に関する機能要件コンポーネントとして、IT 環境のセキュリティ機能要件 **FTP_ITC_EX_IMP.1** を設けている。これら TOE のセキュリティ機能要件と IT 環境のセキュリティ機能要件が協調して動作することにより、CC パート２で規定されている **FTP_ITC.1** と同等のセキュリティ機能要件を実現している。
なお、管理要件として、**FTP_ITC_EX_INI.1**、**FTP_ITC_EX_IMP.1** ともに、CC パート２で規定されている **FTP_ITC.1** と同等の要件を規定しているが、本 ST では、FMT クラスを選択していないため、管理すべき項目ではない。
また、監査要件として、**FTP_ITC_EX_INI.1**、**FTP_ITC_EX_IMP.1** ともに、CC パート２で規定されている **FTP_ITC.1** と同等の要件を規定しているが、本 ST では、FAU_GEN を選択していないため、監査要件として記録すべき項目ではない。
さらに、依存性についても、**FTP_ITC_EX_INI.1**、**FTP_ITC_EX_IMP.1** ともに　なし　としているが、これも CC パート２で規定されている **FTP_ITC.1** と同等である。

8.2.2. 最小機能強度レベル根拠

本 TOE は、第 3 章 TOE セキュリティ環境で述べたように、組織のセキュリティポリシーを実現する製品であり、脅威は想定していない。従って、最小機能強度レベルは、SOF-基本が妥当であるといえる。また、本 TOE において、確率的または順列的メカニズムに基づくセキュリティ機能要件は選択していない。従って一貫している。

8.2.3. セキュリティ機能要件依存性

セキュリティ機能要件のコンポーネントの依存性を表 8-3 に示す。

表 8-3 セキュリティ要件のコンポーネントの依存性

セキュリティ機能要件	CC Part2 で規定されている依存コンポーネント	充足性
FDP_DAU.1	なし	―
FTP_ITC_EX_INI.1	なし	―
FCS_COP.1	[**FDP_ITC.1** または **FDP_ITC.2**	※1
	または **FCS_CKM.1**]	※2
	FCS_CKM.4	○
	FMT_MSA.2	※3
FCS_CKM.4	[**FDP_ITC.1** または **FDP_ITC.2**	※1
	または **FCS_CKM.1**]	※2
	FMT_MSA.2	※3
FTP_ITC_EX_IMP.1	なし	―

※1 : **FDP_ITC.1**、**FDP_ITC.2** は、TSC 外からの利用者データのインポートに関する要件であるが、TSF が確実に動作する上で、IT 環境の TSC 外からインポートしたデータに対するアクセス制御および情報フロー制御は必要としておらず、TOE は IT 環境に対してこの機能要件を要求しない。従ってこの要件は適用しない。

※2 : **FCS_CKM.1** は、鍵の生成に関する要件であるが、第 2 章で記述したが、XML 署名の付与および検証で使用する電子証明書は、TOE の範囲外である認証機関で発行される。
従って、**FCS_CKM.1** は TOE の範囲外であるためこれらの要件を選択しない。

※3 : **FMT_MSA.2** はセキュアな値のみセキュリティ属性として受け入れられることを保証する要件であるが、本 ST で選択した **FCS_COP.1** および **FCS_CKM.4** において利用者によって入力されるセキュリティ属性はない。従って、この要件は適用しない。

8.2.4. セキュリティ機能要件相互補完性
前節より TOE セキュリティ機能要件と IT 環境セキュリティ機能要件は、一部の例外を除き依存関係のある機能要件と相互補完している。
本 TOE で想定する脅威は存在せず、組織のセキュリティポリシーを実現するためのセキュリティ対策方針は、署名の付与／検証に関する暗号操作と高信頼チャネルの開始に関するものであり、他のセキュリティ機能要件のバイパスを防ぐ必要はない。
また、セキュリティドメインは単一であり、TOE が想定する脅威も存在しないため、信頼できないサブジェクトからの改ざん、干渉、セキュリティ機能の非活性化を考慮する必要はない。

8.2.5. セキュリティ保証要件根拠
本 TOE の評価保証レベルは、EAL2＋ALC_FLR.1 である。
本 TOE が想定する脅威は存在せず、電子フォームシステムの設計者が EUR Form 帳票に設定するセキュリティポリシーを実現するためにセキュリティ機能を具備している製品である。また、本 TOE の利用者は申請者という多数の一般的な利用者であり、自宅などの通常の環境で利用している。
EAL2 は、このような TOE の特性に対して、構造設計の観点での評価、セキュアな配布手続き、脆弱性評定を含むことから妥当な選択である。
また、昨今、セキュリティ脆弱性問題への対応が重要となってきているため、セキュリティ欠陥の修正を含む ALC_FLR.1 を追加することも妥当な選択である。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能根拠

第 6.1 節 TOE セキュリティ機能の表 6-1 で示したように、各 TOE セキュリティ機能は 1 つ以上のセキュリティ機能要件に対応している。

FDP_DAU.1：

SF.MESSAGE_SIGN、**SF.PARTIAL_SIGN** は、申請者がサーバに送信する申請データ全体および EUR Form 帳票に設定されている部分署名の対象データに対して XML 署名を付与する機能を提供する。これにより、有効性の保証として使用できる証拠を生成する能力を提供している。

SF.PARTIAL_VERIFY は、EUR Form 帳票に設定されている部分署名の対象データに対して XML 署名を検証する機能を提供する。これにより、EUR Form 帳票に設定されている部分署名の対象データに対する有効性の証拠を検証する能力を提供している。

FTP_ITC_EX_INI.1：

SF.INITIATE_HTTPS は、当該電子フォームシステムのセキュリティポリシーとして既定されていた場合、申請データを送信するために、送信先のサーバとの間で HTTPS 通信を開始する。

以上により、すべての TOE セキュリティ機能要件が必要とする機能を、TOE セキュリティ機能が提供していることが示される。

8.3.2. セキュリティ機能強度根拠

本 TOE の最小機能強度レベルは、SOF-基本であるが、本 TOE において、確率的または順列的メカニズムに基づくセキュリティ機能要件がないという主張、および SOF 主張を実現すべき IT セキュリティ機能はないという主張で一貫している。

8.3.3. セキュリティ保証手段根拠

第 6.3 節 保証手段の表 6-2 に示したように、EAL2 および ALC_FLR.1 で必要とするすべての TOE セキュリティ保証要件に対して、保証手段を対応付けている。また、保証手段によって、本 ST で規定した TOE セキュリティ保証要件が要求する証拠を網羅している。従って EAL2＋ALC_FLR.1 における TOE セキュリティ保証要件が要求している証拠に合致している。

8.4. PP 主張根拠

本 ST では、PP との適合を主張しない。